REMARKS

Claims 1-20 were pending in the application prior to this action. The Examiner rejects claims 1 and 9 under 35 U.S.C. § 102(e) as being anticipated by Holmes et al (U.S. Pat. No. 6,334,056 B1). The Examiner rejects claims 2-8 and 10-20 under 35 U.S.C. § 103(a) as being unpatentable over Holmes in view of Nevoux et al (U.S. 5,661,806A).

The applicants amend claims 1, 9, and 16.

The application remains with claims 1-20.

The applicants add no new matter and request reconsideration.

Claim Rejections - 35 U.S.C. §102 and § 103

Claim recites *an access point...to authenticate the wireless device without going through the firewall.* Claim 9 recites *an access means...to authenticate the wireless means without going through the firewall means.* Claim 16 recites *validating the access point... without going through a firewall means.* In each instance, the system validates the wireless device and/or access point without going through the firewall since the access point and, thus, the wireless device, are coupled directly to the wired LAN as shown in Figure 2. Put differently, the access point need not be authenticated by the firewall to gain access to the wired LAN since it is directly coupled to the wired LAN and need only seek authentication by the separate authenticating server *without going through the firewall.* This allows the wireless LAN to be integral to the wired LAN reducing cost and installation labor as well as improving access speed as we describe in the application's specification.

Holmes, on the other hand, discloses a system in which "all traffic to and from the intranet passes through this firewall" 32. Holmes, column 4, lines 14-15. Holmes discloses a system in which the firewall identifies the incoming URL as coming from a known wireless provider. Holmes, column 5, lines 3-10. In short, Holmes discloses a system in which all traffic must pass through the firewall 32 for initial authentication since it is integral to the router 30 alleged by the Examiner as disclosing the access point recited. The Examiner cannot identify the router 30 as authenticating the wireless device (or means) *without going through the firewall* when the firewall 32 embedded in the router 30 is the device actually performing the authentication as described in e.g., column 4, lines 4-18.

Claim 1 recites *an authentication server...to provide the operator with access to the wired LAN after authenticating the access point, the wireless device, and the operator without*

going through the firewall. Claims 9 and 16 include similar limitations. As before, the claims recite that authentication occurs at an authentication server distinct from and without going through the firewall. In contrast, Holmes discloses a system in which all traffic moves, at least temporarily, through the firewall 32 embedded in the router 30.

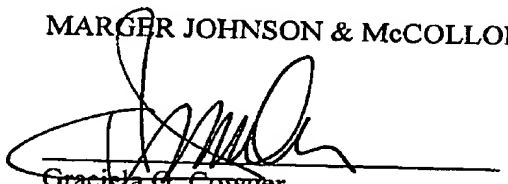
Even if Holmes' server 34 discloses the recited authentication server —an untenable position as we describe above—, the server 34 does not authenticate the access point, the wireless device, *and* the wireless operator as recited in claims 1, 9, and 16. Rather, the server 34 only authenticates the wireless operator by requesting a valid user id and password. Holmes Figure 3 and column 5, lines 13-26.

Conclusion

The applicants request reconsideration and allowance of all claims. The applicants encourage the Examiner to telephone the undersigned at (503) 222-3613 if it appears that an interview would be helpful in advancing the case.

Respectfully submitted,

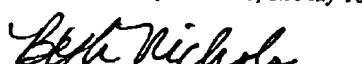
MARGER JOHNSON & McCOLLOM, P.C.



Graciela G. Cowger
Reg. No. 42,444

MARGER JOHNSON & McCOLLOM, P.C.
1030 SW Morrison Street
Portland, OR 97205
(503) 222-3613
Customer No. 20575

I hereby certify that this correspondence is being transmitted to the U.S. Patent and Trademark Office via facsimile number (703) 872-9306, on May 10, 2004.

Signature 
Beth Nichols